REMARKS

Applicant thanks the Examiner for the careful consideration given to this application. Reconsideration and allowance are now respectfully requested in view of the amendment above and the following remarks. Claims 1-2 and 4-18 are pending in this application. Claims 1, 5, 14 and 18 are independent claims. Claims 1, 2, 3-14, 17 and 18 are amended.

Claim Rejections Under 35 U.S.C. §103

Claims 1-2, 4-9 and 12-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,604,807 to Yamaguchi et al. (hereinafter "Yamaguchi") in view of "Transparent Network Security Policy Enforcement," Keromytis et al. (hereinafter "Keromytis") and in view of U.S. Patent No. 6,775,769 to Inada et al. (hereinafter "Inada"). This rejection is respectfully traversed.

Applicants submit that the combination of Yamaguchi, Keromytis and Inada does not teach or suggest the combination of elements recited in the pending claims. Independent claim 1, in part, recites "a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption." Claims 5, 14 and 18 recite similar features. Yamaguchi does not teach or suggest these features.

The Office Action acknowledged that Yamaguchi does not teach or suggest inputting "into each of the encryption apparatus and the communications terminals having encrypting capability, the information including whether or not data packets are to be discarded between specific terminals after the data packets have been received." However, the Office Action alleged that Yamaguchi discloses inputting "into each of the encryption apparatus and the communications terminals having encrypting capability, the information including … a time period for the encryption."

Col. 13, line 60-Col. 14. line 12 of Yamaguchi discloses that

> Thus, according to this second embodiment, the cipher communication between the client 53 and the server 55 through the network 52 is realized by first

> connecting the cipher gateway device 54 between the network 52 and the server 55, such that, prior to the establishment of the session between the client 53 and the server 55, the session key is obtained from the key distribution center 51 by the cipher gateway device 54 in response to the cipher communication request from the client 53, and the obtained session key is distributed to the client 53 so that the common session key is shared by the client 53 and the cipher gateway device 54, and then establishing the session between the client 53 and the server 55 at a timing of the cipher synchronization between the client 53 and the cipher gateway 54. Here, the communication between the cipher gateway device 54 and the server 55 can be the non-cipher (plain text) communication. Consequently, it is possible to provide a cipher communication system and scheme capable of realizing the cipher communication without affecting the already existing application programs and hardware. (underlining added)

Although Yamaguchi discloses that the session is established between the client and server at a timing of cipher synchronization between the client and the gateway, this is not equivalent to inputting "into each of the encryption apparatus and the communications terminals having encrypting capability, the information including … a time period for the encryption," as recited in the pending claims. There is no teaching or suggestion in Yamaguchi that the session key transmitted from key distribution center to the gateway and later transmitted from the gateway to the client includes "a time period for the encryption." Instead, as disclosed in Yamaguchi, the session key transmitted from the key distribution unit is for enciphering/deciphering text between the gateway and the client. The only disclosure of timing noted in the cited sections of Yamaguchi is that the session is established between the client and server at a timing of cipher synchronization between the client and the gateway. Establishing a session between the client and server, by the gateway, at a timing of cipher synchronization between the client and the gateway, as disclosed in Yamaguchi is not equivalent to receiving, at the gateway, information including "a time period for encryption," as the Office Action seems to suggest.

The Office Action also acknowledged that Yamaguchi does not teach or suggest that "the encryption apparatus further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process is performed," as recited in claim 1. Claims 5,

14 and 18 recite similar features. However, the Office Action cited Keromytis to cure this deficiency.

Keromytis discloses that network bridges transparently connect two or more LAN segments by storing a frame received from one segment and forwarding it to another segment. See the first sentence of Section 1 of Keromytis. Keromytis discloses an Ethernet bridge that also provides IP filtering capability. As Ethernet frames pass through the bridge, they are examined to see if they carry IP traffic. If not, the frame is just bridged. If the frame includes IP traffic, the Ethernet header is removed from the frame and copied and the resulting IP packet is passed to a subroutine which notifies the bridge whether the packet is to be forwarded or dropped. The Ethernet header of the frame under examination is appropriately modified on the frame to be forwarded, and the resulting frame is bridged. See the second paragraph of Section 1 of Keromytis. Network layer encryption, typically in the form of IPsec, is used to protect traffic between networks, hosts and users. In a virtual LAN, Ethernet frames are encapsulated inside IPsec packets and then transmitted to a remote device which removes the protection and forwards the frames to the local LAN. Alternatively, in a "bump in the wire" configuration, a bridge transparently implements IPsec on behalf of one or more hosts. See Section 3 of Keromytis.

Keromytis does not teach or suggest that "the encryption apparatus further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process is performed," as recited in the pending claims. Keromytis discusses general network bridges. However, there is no teaching or suggestion that the bridge discussed in Keromytis is part of an encryption apparatus. Instead, Keromytis discloses several methods of using IPsec in a bridge, none of which discloses bridging "output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process is performed," as recited in pending claims. (underlining added)

As noted above, the Office Action acknowledged that Yamaguchi does not teach or suggest "a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information

including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received." However, the Office Action alleged that Inada cures this deficiency.

Inada discloses multiple filters, such as a ciphertext output filter, a home station output filter, and a plaintext output filter. Each of these filters is for filtering a packet transferred to an associated port and for determining if the packet is to be discarded. None of the filters of Inada is inputted from an manager terminal "into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received." Instead, the filters of Inada appear to be static components of the cryptographic apparatus. Therefore, Inada also does not teach or suggest inputting "into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received," as recited in the pending claims.

Based on the distinctions noted above, Applicants submit that the combination of references does not teach or suggest the combination of elements recited in claims 1, 5, 14 and 18. Each of claims 2, 4, 6-13 and 15-17 depends on claims 1, 5 and 14, and incorporates all of the elements of claims 1, 5 and 14, in addition to the further elements recited in claims 2, 4, 6-13 and 15-17. Hence, claims 2, 4, 6-13 and 15-17 include features not disclosed in the cited references at least because of their dependence on claims 1, 5 and 14. Therefore, Applicants respectfully request that this rejection of claims 1-2, 4-9 and 12-18 under 35 U.S.C. §103 be withdrawn.

Claims 10-11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,604,807 to Yamaguchi in view of Keromytis and in view Inada and in further view of U.S. Patent No. 5,481,610 to Doiron (hereinafter "Doiron"). This rejection is respectfully traversed.

Dorion dues not cure the deficiencies of Yamaguchi, Keromytis and Inada, as noted above. Therefore, Applicants respectfully request that this rejection of claims 10-11 under 35 U.S.C. §103 be withdrawn.

Disclaimer

Applicants may not have presented all possible arguments or have refuted the characterizations of either the claims or the prior art as found in the Office Action. However, the lack of such arguments or refutations is not intended to act as a waiver of such arguments or as concurrence with such characterizations.

CONCLUSION

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

The Office is authorized to charge any necessary fees to Deposit Account No. 22-0185.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 27592-01101-US1 from which the undersigned is authorized to draw.

Dated: September 23, 2009

Respectfully submitted,

Electronic signature: /Arlene P. Neal/
Arlene P. Neal
Registration No.: 43,828
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant